Cybercrime, money mules and situational crime prevention

Leukfeldt, E. Rutger; Kleemans, Edward R.

published in
Criminal Networks and Law Enforcement
2019

document version
Publisher's PDF, also known as Version of record

5 Cybercrime, money mules and situational crime prevention

Recruitment, motives and involvement mechanisms

E.R. (Rutger) Leukfeldt and
E.R. (Edward) Kleemans

5.1 Introduction

> OK, I will tell you the truth. I don't want to lie about it. I was contacted several times a day by a guy asking for my cash card and PIN-code. I was supposed to get something in return. At that time, I had serious problems. Although I refused several times, eventually I gave him my cash card. After all, there was no money in my bank account and I would get some money in return.

This quote from an interrogation shows how a money mule was recruited for a cybercriminal network. The offenders put money, stolen from victims of phishing or banking malware, into this bank account. The money trail to the offenders is interrupted by withdrawing the money from the account of the money mule directly after the money has been transferred to this bank account. Therefore, money mules are an important part of the crime script of criminal networks involved in committing financial cybercrimes, such as phishing and malware. However, as this section shows, little empirical research on money mules has been carried out. This chapter, therefore, adds to the literature by providing insight into recruitment processes of money mules and the motives and neutralisation techniques of money mules.

Phishing is the process aimed at tracing users' personal information by criminals posing as a trusted authority and thereby using digital means, such as e-mail (see, e.g. Lastdrager, 2014, who analysed 113 definitions of phishing). Crime scripts of phishers differ, but phishers usually use e-mails that appear to be sent by a bank to gain login credentials of victims (see, for various examples, Leukfeldt et al. 2017a, 2017b). The e-mail is, for example, about the security of the online bank account of the victim and immediate action is required. The victim is persuaded to click on a link in the e-mail to solve the security problem. The link leads to a phishing website which appears to be from the bank. Once the victim logs on to the website, the criminals obtain his or her credentials. In order to transfer money from the victim's account, the criminals have to obtain transaction authentication codes. The next step, therefore, is to telephone the victim.

A criminal calls the victim and poses as a bank employee who wants to finalise the security update of the online bank account and needs security codes to do so. Depending on the bank of the victim and type of transaction authentication method used by the bank, the victim has to generate a code, which is abused by the criminals to transfer money. The money is not transferred to members of the criminal network, but to money mules. Money from the money mule accounts is cashed as soon as possible. These money mules are not directly linked to the members of the criminal network and are used to obscure the trail to the criminal network.

The crime script of networks using malware is slightly different. Malware is short for malicious software. This software is used by criminals to intercept users' personal information in an automated way. Once the computer of the user is infected with the malware, the criminal gains control over this computer. An infection is started, for example, by opening an infected attachment of an e-mail. Once the criminals control the victim's computer, criminals are able to manipulate online banking sessions and send money to accounts of money mules. Again, money mules play an important part in this crime script.

Money mules, therefore, are not part of the group of core offenders coordinating the illicit activities. Nevertheless, they are a crucial part of the crime script, as they interrupt the money trail while at the same time the core offenders are able to reap their profits anonymously. They take a high risk for a relatively low reward and enable cybercriminal networks to operate smoothly. Surprisingly, hardly any empirical research has been done into money mules. Scholars acknowledged decades ago that criminals abuse Information and Communication Technology (ICT) to commit crimes (for example, Aston et al. 2009; Loch et al., 1992; Akdeniz, 1996; Wall, 1997; Mann and Sutton, 1998; Gattiker and Kelley, 1999; Capeller, 2001; Grabosky, 2001; Grabosky and Smith, 2001) and more recently the nature and functioning of cybercriminal networks are gaining more and more attention (for example, Peretti, 2008; Holt and Lampke, 2010; Lu et al., 2010; Décary-Hetú and Dupont, 2012; Lusthaus, 2012; Soudijn and Monsma, 2012; Yip et al., 2012; Afroz, 2013; Leukfeldt, 2014; Leukfeldt et al., 2017a, 2017b, 2017c, 2017d). Furthermore, several studies acknowledge the important role of money mules in the diversion of money stolen by cybercriminals who are engaged in financial cybercrimes (Choo, 2008; Moore and Clayton, 2007; Aston et al., 2009; McCombie, 2011; Soudijn and Zegers, 2012; Leukfeldt, 2014; Leukfeldt et al. 2017a, 2017b, 2017c, 2017d). These studies, however, concentrate primarily on the core of criminal networks and the role of money mules within these cybercriminal networks remains underexposed.

The crucial function of money mules in the crime scripts of phishing and malware networks makes this specific group extremely relevant for situational crime prevention. If it is hard to carry out these illicit activities without money mules, they are an obvious target for situational crime prevention, e.g. by making it harder to recruit money mules, by making it less attractive to be a money mule or by removing excuses. Removing excuses is one of the strategies of situational crime prevention (e.g. Cornish and Clarke, 2003), but can also be traced back to

the techniques of neutralisation (Sykes and Matza, 1957; for a review of empirical research see Maruna and Copes, 2005). The interrogation we mentioned in the introduction illustrates various excuses for cooperating as a money mule: he only agreed after several refusals, he had serious problems and needed extra money, and after all, there was no money in his bank account. More insight into the nature of these excuses could help design effective intervention strategies.

This chapter explores the possibilities for situational crime prevention regarding the recruitment of money mules. Section 5.2 contains a brief description of situational crime prevention, the theoretical angle of this chapter. Section 5.3 analysed the data and methods of 14 Dutch criminal investigations into cybercriminal networks to get insight into the motives and techniques of neutralisation of money mules. Section 5.4 takes the perspective of the recruiters and answers the question of how recruiters find money mules, e.g. by using social contacts and/or specific offender convergence settings. Section 5.5 focuses on the motives and techniques of neutralisation used by money mules. Section 5.6 presents the main conclusions and opportunities for situational crime prevention.

5.2 Strategies for situational crime prevention

Situational crime prevention strategies encompass a wide range of opportunity-reducing measures aimed at hindering or preventing crime. Originally, Clarke (1980) distinguished two potential strategies: reducing the physical opportunities for offending and increasing the chances of an offender being caught. Over the years, strategies and methods were elaborated and adapted in response to new empirical research (see, e.g. Clarke, 1997; Clarke and Homel, 1997; Cornish and Clarke, 2003). At this moment, five different strategies for situational crime prevention are recognised:

- Increase the effort of crime (e.g. target hardening by installing better locks);
- Increase the risk of crime (e.g. extend guardianship by neighbourhood watch);
- Reduce the rewards of crime (e.g. remove targets or identify property);
- Reduce provocations that invite criminal behaviour (e.g. neutralise peer pressure);
- Remove excuses for criminal behaviour (e.g. set rules about (un)wanted behaviour).

Based on these five strategies for situational crime prevention, Cornish and Clarke distinguish 25 techniques for situational crime prevention. According to these authors, this 'classification of crime prevention techniques is designed to provide a conceptual analysis of situational strategies, and to offer practical guidance on their use in reducing criminal opportunities' (Cornish and Clarke, 2003, p. 41).

The primary focus of these 25 techniques for situational crime prevention was opportunistic street-level crime. Only later on was the situational crime prevention theory transplanted to other, more serious types of 'organized crimes'

(e.g. Cornish and Clarke, 2002; Bullock et al., 2010; Kleemans and Soudijn, 2017). However, situational crime prevention cannot only be applied to offline crime, but also to online crime. Hartel et al. (2011) review the literature and show that principally these techniques are equally applicable to cybercrime. Examples include increasing the effort of crime by using password-protected files, increasing the risk of crime through extended guardianship by Internet service providers who filter e-mails, reduce the rewards of crime by encrypting valuable data, reduce provocations that invite criminal behaviour by discouraging imitation by prompting software patching, and remove excuses for criminal behaviour by posting instructions and making the general public aware of the consequences of crime.

When we focus on money mules, we might interpret them as 'facilitators' or 'enablers,' as these persons carry out three essential functions: they make it possible to transfer the stolen money to a bank account, they make it impossible to trace the core members of the criminal network and they enable these offenders to withdraw the cash from the bank account. At the same time, they run a high risk to be caught and they receive a relatively low reward. How do core members recruit these money mules? Do they use traditional offline social contacts, online contacts, digital offender convergence settings such as forums, et cetera (e.g. Leukfeldt, 2014; Leukfeldt et al. 2017a, 2017b)? And what are the motives and techniques of neutralisation of these money mules? These questions will be answered in Sections 5.4 and 5.5.

5.3 Data and methods

Fourteen Dutch criminal investigations into cybercriminal networks were analysed to get insight into motives and techniques of neutralisation of money mules. The investigations lasted six months to three years and were carried out in the period 2004–2014. The investigations show that often hundreds of money mules are used by these cybercriminal networks (for example, because the investigations show to which money mules the money is transferred from the victims' bank accounts). However, the number of interrogated money mules is much lower. One reason for this is that investigations are not always focused on money mules, but on core members or important enablers. Another reason is that tracing and interrogating all money mules is too time-consuming. Therefore, the number of interrogated money mules varies for each investigation.

The 14 analysed investigations contained interrogations of 211 money mules. Four investigations included two to 10 interrogated money mules, six investigations included 11 to 20 interrogated money mules, and three investigations contained 20 or more interrogated money mules. Not all interrogations of these 211 money mules yielded enough information for this analysis: 69 suspects did not cooperate during the interrogation ('no comment') and 30 claimed to be innocent. The other 112 money mules admitted to having assisted in cashing the money that was stolen by phishing or malware attacks. The analysis of this chapter focuses on these 112 interrogations.

This chapter does not include all forms of cybercrime. There are simply too many types of cybercriminal networks with major differences between them, ranging, e.g. from networks that threaten banks or major online retailers to shut down their websites or online systems to groups engaged in producing and distributing child pornography. This study is part of the Research Programme on Safety and Security of Online Banking. Therefore, this study only includes money mules which are used by groups carrying out attacks on online banking. That boils down to phishing attacks and malware attacks. In literature, different definitions for phishing are presented (see, for example, Lastdrager, 2014). The scope of these definitions is as follows: Phishing is the process aimed at retrieving users' personal information by criminals posing as a trusted authority and thereby using digital means, such as e-mail. As mentioned before, a criminal, for example, sends an e-mail that seems to come from a trusted third party such as a bank. The e-mail refers to a problem with the online bank account of the user (e.g. 'A security upgrade is needed') coupled with the request to take immediate action to resolve the issue (e.g. 'Log in using the link in the e-mail to update the security of your account'). The aim of the attack is to intercept user credentials. User credentials can also be intercepted in a more technological way. Criminals use malware – or malicious software – such as viruses, worms, Trojan horses and spyware, to intercept credentials or manipulate entire online banking sessions.

The 14 police investigations are not publicly available. The Public Prosecution Office ('College van PG's') must give permission for the scientific analysis of a police investigation, and the research proposal must first be assessed by the Research and Documentation Centre (WODC) of the Dutch Ministry of Security and Justice. WODC gives advice on the (scientific) quality of the research proposal and the research topic (e.g. added value regarding current research projects).

It was decided to use investigations into criminal networks which had been completed by the police. Completed means that the investigation team has collected enough evidence for the public prosecutor to decide to prosecute the suspects. There may not necessarily have been a ruling by a judge yet. Excluding cases where no judgment is yet available would mean that only a few cases would remain because it may take years before suspects are convicted (after appeal) (Kleemans, 2014).

There is no central registration system in the Netherlands that allows for a quick overview of all criminal investigations into phishing networks. The selection of cases was, therefore, carried out by using the snowball method. Starting points were cybercrime and fraud teams on a national and (inter)regional level. Using existing contacts within the Dutch police, the Police Academy and Public Prosecutors, team leaders and senior investigators of these teams were asked whether they knew any investigations into networks using phishing or malware to attack users of online banking. Furthermore, an online database in which court documents are published was used and a media analysis was done to find news reports about relevant cases. During the file study, law enforcement officers and public prosecutors involved in the criminal investigation were asked whether they knew of any other phishing cases.

5.4 The recruitment of new money mules

Although not all interrogations of money mules have detailed information about their financial situation – sometimes police officers simply do not ask any questions about this – the majority of the 112 money mules seem to have limited financial funds. At least 40 money mules are still in high school or university and only have part-time jobs, five others quit school and have a part-time job, 35 money mules are out of work and rely on benefits and 58 claim to be in debt. Recruiters seem to make use of this vulnerability. They promise potential money mules a financial reward for little effort, namely offering their bank accounts for a fee.

In 13 out of 14 investigations into phishing and banking malware networks, money mules are recruited through existing social contacts. Core members or recruiters (used by these networks) contact people they know from their own neighbourhoods, schools or sports clubs. They ask questions about the financial situation of potential money mules, or they ask frankly if they want to earn easy money. Box 1 includes some examples.

Box 1 Recruitment through social contacts

'I knew the recruiter from soccer. I played soccer against his team once in a while. I also know him from nightlife, apart from that I did not meet him on a regular basis. He's not a friend of mine, but I do occasionally meet him. I didn't have too bad an impression of him. I've also never met him at home. He asked several times for a cash card. Eventually, I just gave it to him.'

'I knew her through my niece, she attended the same school. She's not really my niece. I know her all my life, so she's just like a niece to me. We originate from the same country and our parents also know each other. This way, I actually came into contact with them. And, as a result, I was introduced to other people again and again. This all happened at a school in the Bijlmer-neighbourhood in Amsterdam.'

The networks that do not recruit through direct social contacts have to find potential money mules through other ways. An example is posting advertisements on job websites, as described in studies by Aston et al. (2009) and McCombie (2011). On these websites, recruiters are able to target people looking for work. In one of the analysed investigations, money mules are recruited in a similar way (see Box 2). In this case, money mules are recruited through e-mails that were sent on a massive scale. These e-mails asked for employees for a financial company. This company also wants to service Dutch clients and is, therefore, looking for a new employee who wants to offer his or her bank account to put money into. These payments need to be transferred to a third party. The 'employees' are allowed to keep a commission regarding this payment.

Box 2 Recruitment through spam

The e-mail with a fake job description promises a guaranteed salary of 2000 US dollars. A police agent enrols as a new employee through the website mentioned in this e-mail. The next e-mail by this 'company' includes a labour contract that needs to be filled out and sent back to the company. Furthermore, the e-mail explains again the earnings (5% of the transferred money) and that the money needs to be transferred through Western Union. After the signed contract has been sent back, a second e-mail follows asking for the bank account number, type of account (business or private), transfer limits, and IBAN and SWIFT numbers. After answering this e-mail, a third e-mail follows stating that 9,447 Euro has been transferred. The employee is entitled to keep 473 Euro. The rest has to be transferred to two persons in Russia through Western Union. Furthermore, the e-mail mentions that after the transfer, specific data of this transaction need to be e-mailed to this company. If any travel costs are involved because the Western Union office is not nearby, employees get 100 Euro per 100 kilometres.

5.5 Motives and techniques of neutralisation

During interrogations, money mules make different statements about why they assisted in transferring money. Not all suspects admit to having participated deliberately, and others refuse to cooperate with the interrogators. Interrogations yielding information about motives of money mules, however, show various motives and techniques of neutralisation that will be described below. They are described separately, but in reality, they can appear in various combinations.

One group of money mules admits to having cooperated knowingly and deliberately with the fraudulent money transfers and that they couldn't resist the lure of earning easy money. Many of these money mules are part of a subculture in which it is normal to cooperate with these kinds of fraudulent activities and say they feel pressured by recruiters to collaborate. Next to that, there are various money mules who admit to having cooperated, yet state as an excuse that they were not aware that these activities were fraudulent. For example, because they thought that the money transfers have a legitimate purpose or that virtual money would not imply real victims. A third group blames the victims. Examples of these motives of money mules will be described below.

5.5.1 Subculture

Statements of 26 money mules show they are part of a subculture in which it is normal to cooperate with such fraudulent activities. Several money mules claim during interrogations that it is relatively normal that they were approached by people who asked them to lend them their cash card (see Box 3).

Box 3 Subculture

During an interrogation, Suspect 38 states: 'I get text messages on a regular basis from several guys. These guys ask me if I know anyone who wants to make money. They simply ask you if you have cash cards.' Suspect 38 shows a text message that she got that morning from F: 'Don't you know a girl who wants booty?'

'Since about 2 years rumour has it that you can earn easy money by providing your bank account. Also through the Internet messages are sent that you can earn money by offering your bank account. I didn't want to cooperate, I am not a money mule or errand-boy. Some months ago I changed my mind. I really could use the money. I ran into a Surinamese boy and he introduced me to S1.'

Suspect 9 states: 'This is general knowledge in Amsterdam. It's a big hit. They do it with everything. They earn a lot of money with fraud.' About the person to whom she would have offered her cash card, she states: 'They call him Prince. It's from the streets. Really, everybody knows him. He's from Ghana. Together with his uncle he commits fraud (…) I said already that everybody in the Netherlands is involved. Many people do it. Especially youngsters. You can earn easy money and many want to do that. Many youngsters or junkies who have nothing to lose.'

5.5.2 Earning easy money

Thirty-one money mules state they simply wanted to earn easy money. Examples are described in Box 4.

Box 4 Earning easy money

Suspect 4: 'About two weeks later I went to S15 and he talked about money. He thought his student benefits were too low. He asked if I knew a way to get more money. S15 wanted more money for shoes, caps, and so on. I then told him that you could earn 800 or 900 Euro by offering your cash card. S15 stated that he knew who S9 was, he knew his face. I explained everything about the cash card. S15 asked about problems he might run into. I told him that S9 had communicated that you wouldn't run into problems and that otherwise, you could tell S9's name. S15 wanted to offer his cash card. However, he wanted to be sure he would get that 800 or 900 Euro.'

5.5.3 Looking up to the lifestyle of criminals

Furthermore, the interrogations of 15 money mules make clear that they look up to the lifestyle of core members and recruiters (see Box 5). The members of criminal networks carrying out phishing and malware attacks have a high prestige among local youngsters, and youngsters starting as recruiters suddenly turn out to be able to spend considerable sums of money. They drive luxurious cars, wear fancy clothes and spend lots of money on nightlife. Youngsters fancy earning easy money themselves. They are approached regularly on the streets, at hangouts, during nightlife or at school. Subsequently, contact details are exchanged and the Internet and mobile phones make it easy to maintain contact. Furthermore, other persons are actively approached via text messages on mobile phones. Youngsters get messages asking for cash cards from friends of vague acquaintances ('who wants to earn easy money').

Box 5 Looking up to the lifestyle of criminals

'Not a normal car, a fancy car. It was a dark car, it had been made lower. Sometimes Mercedes and sometimes BMW. The clothes of this guy were from Gucci, they also frequented a club. They were in the secured VIP-area, we were in the crowd. The two of them often were together. One was wearing a Moncler. That's an expensive coat. I've always wanted to have such a coat. Both had golden teeth.'

'In June or July 2012, I became acquainted with a guy (recruiter G). He is a nephew of a friend of my ex-boyfriend. This guy took me out for dinner several times and gave me expensive clothes, for example, a jacket of 500 Euro and shoes of 250 Euro. He also offered me money once in a while to buy something for my son. Recruiter G heard about my financial problems and knew a way to earn easy money. I knew it was about fraud. I had to register as nail stylist at the Chamber of Commerce. First, I didn't want to, but after some encouragement, I eventually agreed to do it.'

5.5.4 Money mules offer their services

One of the consequences of a subculture of youngsters in which core members and recruiters can show off their expensive lifestyle is that new money mules do not always have to be recruited. Potential money mules take the initiative and offer their services because they know they can earn money by providing their cash card and codes (see Box 6). During interrogations, seven money mules admitted to having taken the initiative to offer their services.

Box 6 Money mules offer their services

'I don't remember exactly. I was talking to X and she said that her mother wanted to make money. Apparently, because she went on a holiday, so it should have been before October. (…).With making money, I mean fraud with a cash card. After that talk I asked X if he knew such people. X said that he actually knew such people. I told this to her and she communicated that with her mother.'

5.5.5 Pressure from recruiters

Five other money mules state that in the end they couldn't stand the pressure from recruiters, they knew they could earn easy money by providing their bank accounts and they were frequently approached to collaborate. They claim they refused at first, but after some time they gave in due to the pressure of recruiters (see, for example, Box 7).

Box 7 Pressure from recruiters

'Actually, I hardly ever saw these guys. I had never seen them before. Suddenly, I saw them more frequently. Every time I was in the city, I ran into them. They often hang out with their cars near the Hema [a department store]. There I ran into them when I was walking to the train station. Nine out of ten times they approached me. They asked me if I still hadn't fixed it. That small guy asked me that and he told me I could earn a lot. I noticed that he took a pile of banknotes out of his pocket. Most banknotes were 50 Euro and some 100 Euro.'

5.5.6 Excuses: Legitimate transactions

Several money mules claim to be unaware that they were collaborating with crimes victimising other people. Thirty money mules state that they thought the money transactions served a legitimate goal (Box 8).

Box 8 Legitimate transactions

'I ran into him by coincidence. This was close to the Bijenkorf [a luxurious department store] in the city centre of Amsterdam. I saw that he was with S9. I heard that S11 asked me if he could use my account to transfer money from Congo. This would be from his family. I asked him why he didn't take care of that himself. He told me then that he had lost his cash card and that he needed it already today or tomorrow. I asked him how much it was.

He said he wasn't sure, possibly 2000 Euro. His family in Congo was rich according to him.'

'About March 2013, I met S1. I met him at C1000 [a supermarket] … I knew S1 from the McDonalds where I used to work in the past. S1 asked me if I could help him. S1 had lost his identity papers and therefore could not apply for a new cash card. He now had a problem, as his uncle in Turkey would transfer 5000 Euro to his bank account. Because he didn't have a cash card, he could not withdraw this money. S1 now wanted to transfer the money to my account, so I could withdraw it for him. I asked S1 to call this uncle in Turkey and spoke to him myself. The man told me indeed that he would transfer money from Turkey to my account. I trusted S1 and agreed. After we had agreed that his uncle would transfer the money, we went our own ways.'

5.5.7 Excuses: Victimless crimes

Other excuses comprise statements that money mules thought that the activities would be victimless. The statements of two money mules point in this direction. One of these statements is described in Box 9.

Box 9 Victimless crimes

'Subsequently, I got a message from recruiter 2 with the text: "I know somebody who works at the breakdown service of bank X and he could organise some kind of breakdown that makes it possible that virtual money, that is money being circulated around bank accounts in order to earn as much interest as possible, so to say pops up as your balance and we could nibble off a bit discretely which would yield me and you something nice." I thought OK, I can make some money. I didn't have the impression that this was fraud or crime.'

5.5.8 Excuses: Blaming victims

Thirteen money mules blame victims as an excuse. This involves only money mules recruited through spam (see Section 5.7). Box 10 gives an example of such a statement.

Box 10 Blaming victims

'I don't feel responsible because I think the companies are to blame.' This money mule points to the companies from which money was transferred. 'They apparently have bad security that this can happen.'

5.6 Conclusion and possibilities for situational crime prevention

This section focuses on the possibilities for situational crime prevention. The introduction shows that money mules are an important part of the crime script of phishing and malware networks. They interrupt the money trail while at the same time the core offenders are able to reap their profits anonymously. They take a high risk for a relatively low reward and enable cybercriminal networks to operate smoothly. Therefore, we will first present the main conclusions regarding the reasons mentioned by money mules to get involved in money transfers. Subsequently, opportunities for situational crime prevention will be discussed.

Motives and techniques of neutralisation can be distinguished into two categories. The first category comprises money mules who are part of a subculture in which it is normal to collaborate with fraudulent money transfers. Factors that stand out are earning easy money, looking up to the lifestyle of criminals, money mules offering their services and pressure from recruiters. Various motives contribute to the decision to facilitate activities that are obviously fraudulent. The second category refers to techniques of neutralisation and refers to money mules pointing to excuses for their behaviour: the money transfers had a legitimate goal, there were no real victims (as it relates to virtual money) or victims themselves are to blame (as they should have invested more in their own security).

Two situational crime prevention strategies might be suited for making recruitment of money mules more difficult. The first one is to reduce provocations that invite criminal behaviour, especially the measures of reducing peer pressure and imitation. The analysis shows that social ties and peer pressure are important for the recruitment of money mules. Criminal networks recruit new money mules via their own social networks. Potential money mules are, for example, approached on the streets, in hangouts, during nightlife, at sport clubs and in schools. Money mules often claim that everybody in their community knows about frauds being committed, that it is normal to be asked to cooperate, that they are approached to cooperate frequently and that criminals who are involved in phishing and malware have an enviable lifestyle. After a while, money mules offer themselves to the criminal network, as they have heard the stories of earning easy money and don't want to miss the boat.

The second situational crime prevention strategy is removing excuses for criminal behaviour, especially the measure of making potential money mules aware of criminal behaviour. Some money mules claim that they thought they were facilitating a legitimate transaction. Others think that there are no victims, or that the victims are to be blamed, as they have exposed themselves to these risks.

With regard to both strategies, awareness campaigns aimed at potential money mules can be developed. First, potential money mules have to be made aware that they are cooperating with criminals who steal money from innocent people. Second, it should be communicated clearly that money mules are used by criminals to lead law enforcement away from the criminals and towards the money mules. In a way, money mules are victims too. The consequences for money

mules go beyond getting arrested; banks hold the money mules responsible for the money that was stolen from victims. Money mules, therefore, have to pay back the money to the bank, leaving them with the consequences of the crime instead of the core members of criminal networks.

5.7 Limitations

This is a first exploratory study into possibilities to counter the recruitment of money mules, based on 112 statements of money mules from 14 Dutch criminal investigations into phishing and malware networks. This provides unique insights into motives and techniques of neutralisation. However, there are also several limitations.

The analysed statements do not refer to a representative group of money mules. The data relate to suspects that were identified during these investigations and who were interrogated. As investigating money mules is not a high priority, not all money mules have been interrogated. According to police respondents, this is simply impossible as it would take too much time. Furthermore, not all money mules cooperated with the police, so we could only analyse 112 statements of the 211 interrogated money mules, as the other interrogations provided no information about motives.

It is important to note that we cannot fully judge the suspects' statements about motives. Suspects may speak the truth and the police check answers (by cross-examinations and verification questions), but this method also has its flaws. For this study, we put the statements in context, but we had to take the information about motives at face value.

The results of this study may be regarded as a first step in research into money mules. In future research, offender interviews might shed more light on the recruitment processes of money mules and their motives for cooperating with these activities. Furthermore, data from financial institutions might provide quantitative information about background characteristics of money mules. This might also be important to target awareness campaigns.

Acknowledgements

Data for this chapter was collected during the PhD study of the first author. This PhD study was part of the Dutch Research Program on Safety and Security of Online Banking and was funded by the Dutch banking sector, represented by the Dutch Banking Association (NVB), the Police Academy and the Cybercrime Program of the Dutch police.

References

Afroz, S., Garg, V., McCoy, D. & Greenstadt, R. (2013) *Honor Among Thieves: A Common's Analysis of Cybercrime Economies*. San Francisco, CA: IEEE Ecrime Research Summit.

Akdeniz, Y. (1996) Computer pornography: A comparative study of the US and the UK obscenity laws and child pornography laws in relation to the internet. *International Review of Law, Computers and Technology* 10(2), pp. 235–261.

Aston, M., McCombie, S., Reardon, B. & Watters, P. (2009) A preliminary profiling of internet money mules: An Australian perspective. In: *Proceedings of the 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing*. IEEE Computer Society, pp. 482–487.

Bullock, K., Clarke, R.V. & Tilley, N. (eds.) (2010) *Situational Prevention of Organised Crimes*. Cullompton, UK: Willan Publishing.

Capeller, W. (2001) Not such a neat net: Some comments on virtual criminality. *Social and Legal Studies* 10(2), pp. 229–242.

Choo, K.R. (2008) Organised crime groups in cyberspace: A typology. *Trends in Organized Crime* 11(3), pp. 270–295.

Clarke, R.V. (1997) Introduction. In: R.V. Clarke (ed.), *Situational Crime Prevention: Successful Case Studies*. Guilderland, NY: Harrow and Heston, pp. 1–43.

Clarke, R.V. & Homel, R. (1997) A revised classification of situational crime prevention techniques. In: S.P. Lab (ed.), *Crime Prevention at a Crossroads*. Cincinnati, OH: Anderson, pp. 17–27.

Clarke, R.V.G. (1980) Situational crime prevention: Theory and practice. *British Journal of Criminology* 20(2), pp. 136–147.

Cornish, D.B. & Clarke, R.V. (2002) Analyzing organized crimes. In: A.R. Piquero & S.G. Tibbetts (eds.), *Rational Choice and Criminal Behavior: Recent Research and Future Challenges*. New York: Garland, pp. 41–64.

Cornish, D.B. & Clarke, R.V. (2003) Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies* 16, pp. 41–96.

Décary-Hetú, D. & Dupont, B. (2012) The social network of hackers. *Global Crime* 13(3), pp. 160–175.

Gattiker, U.E. & Kelley, H. (1999) Morality and computers: Attitudes and differences in judgments. *Information Systems Research* 10(3), pp. 233–254.

Grabosky, P.N. (2001) Virtual criminality: Old wine in new bottles? *Social and Legal Studies* 10(2), pp. 243–249.

Grabosky, P.N. & Smith, R.G. (2001) Digital crime in the twenty-first century. *Journal of Information Ethics* 10, pp. 8–26.

Hartel, P., Junger, M. & Wieringa, R. (2011) *Cyber-Crime Science = Crime Science + Information Security*. (report) University of Twente.

Holt, T.J. & Lampke, E. (2010) Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies* 23(1), pp. 33–50.

Kleemans, E.R. (2014) Organized crime research: Challenging assumptions and informing policy. In: E. Cockbain & J. Knutsson (eds.), *Applied Police Research. Challenges and Opportunities*. New York: Routledge, pp. 57–67.

Kleemans, E.R. & Soudijn, M.R.J. (2017) Organised crime. In: N. Tilley & A. Sidebottom (eds.), *Handbook of Crime Prevention and Community Safety*. Cullompton, UK: Willan Publishing, pp. 394–406.

Lastdrager, E.E. (2014) Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science* 3(1), pp. 1–10.

Leukfeldt, E.R. (2014) Cybercrime and social ties. Phishing in Amsterdam. *Trends in Organized Crime* 17(4), pp. 231–249.

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.P. (2017a) A typology of cybercriminal networks: From low tech locals to high tech specialists. *Crime, Law and Social Change* 67(1), pp. 21–37.

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.P. (2017b) Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology* 57(3), pp. 704–722.

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.P. (2017c) Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change* 67(1), pp. 39–53.

Leukfeldt, R., Kleemans, E.R. & Stol, W.P. (2017d) The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist* 61(11), pp. 1387–1402.

Loch, K.D., Carr, H.H. & Warkentin, M.E. (1992) Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly* 16(2), pp. 173–186.

Lu, Y., Luo, X., Polgar, M. & Cao, Y. (2010) Social network analysis of a criminal hacker community. *Journal of Computer Information Systems* 51(2), pp. 31–41.

Lusthaus, J. (2012) Trust in the world of cybercrime. *Global Crime* 13(2), pp. 71–94.

Mann, D. & Sutton, M. (1998) Netcrime: More change in the organization of thieving. *British Journal of Criminology* 38(2), pp. 201–229.

Maruna, S. & Copes, H. (2005) Excuses, excuses: What have we learned from five decades of neutralisation research? *Crime and Justice* 32, pp. 221–320.

McCombie, S.J. (2011) Phishing the long line. Transnational cybercrime from Eastern Europe to Australia. PhD thesis. Macquarie University, Department of Computing.

Moore, T. & Clayton, R. (2007) Examining the impact of website take-down on phishing. In: *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit.* Pittsburgh, PA: ACM, pp. 1–13.

Peretti, K.K. (2008) Data breaches: What the underground world of "carding" reveals. *Santa Clara Computer and High-Technology Law Journal* 25(2), pp. 345–414.

Soudijn, M.R.J. & Monsma, E. (2012) Virtuele ontmoetingsuimtes voor cybercriminelen. (Virtual meeting places for cyber criminals). *Tijdschrift voor Criminologie* 54(4), pp. 349–360.

Sykes, G.M. & Matza, D. (1957) Techniques of neutralisation: A theory of delinquency. *American Sociological Review* 22(6), pp. 664–670.

Wall, D.S. (1997) Policing the virtual community: The Internet, cyber crimes and the policing of cyberspace. In: P. Francis, P. Davies & V. Jupp (eds.), *Policing Futures, the Police, Law Enforcement and the Twenty-First Century.* London: Macmillan, pp. 208–236.

Yip, M., Shadbolt, N. & Webber, C. (2012) *Structural Analysis of Online Criminal Social Networks.* ISI 2012, June 11–14, 2012, Washington.